# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-073269
(43)Date of publication of application : 18.03.1997

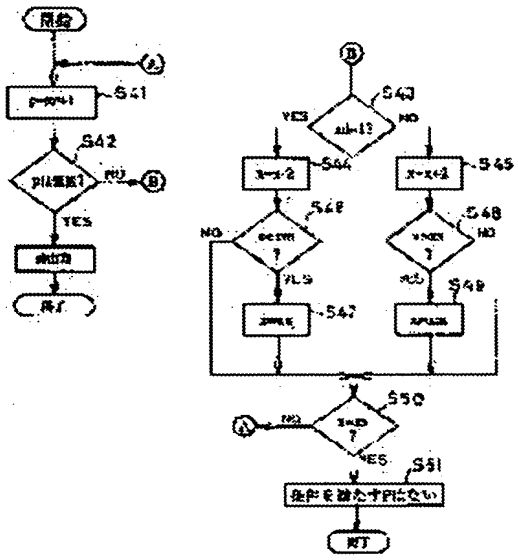
(51)Int.Cl. G09C 1/00
H04L 9/30

(21)Application number : 07-226682
(22)Date of filing : 04.09.1995

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : ABE MASAYUKI
SAITO TAIICHI
UEDA HIROKI

## (54) PRIME NUMBER GENERATOR, PRIME FACTOR DISCRIMINATING DEVICE AND PRIME NUMBER GENERATOR HAVING LIMITATION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a prime number generator, a prime factor discriminating device and a prime number generator having limitation in which prime numbers are generated having a high sefety so that any one of the bit numbers of the prime factors that should be included by P−1 and p+1 becomes less than 1/2 of the bit number of P and the appearance probability of the prime numbers is relatively uniform.
SOLUTION: When a bit number pb of a prime number p, a prime number r which is the prime factor of p−1, a maximum value xx of x, a minimum value xm of x, a final value xs of x, a random number x of an even number in that xm≤x≤xx and a random number xd are externally inputted, compute p=xr+1 and input p into a prime number discriminator. If p is discriminated as a prime number, output p and the process is stopped. If p is discriminated as not a prime number, subtract 2 from x or add 2 to x in accordance with the value of xd. If x becomes less than xm, make x to be xx. If x becomes larger than xx, make x to be xm. If x becomes equal to xs, output a signal indicating that the prime number p which meets input conditions pb and r does not exist and stop. If x in not equal to xs, go back to the first process.



LEGAL STATUS

[Date of request for examination] 21.10.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3292362
[Date of registration] 29.03.2002
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－73269

(43)公開日　平成９年(1997)３月18日

| (51)Int.Cl.[6] | | 識別記号 | 庁内整理番号 | ＦＩ | | 技術表示箇所 |
|---|---|---|---|---|---|---|
| Ｇ０９Ｃ | 1/00 | ６５０ | 7259－5Ｊ | Ｇ０９Ｃ | 1/00 | ６５０Ｚ |
| Ｈ０４Ｌ | 9/30 | | | Ｈ０４Ｌ | 9/00 | ６６３Ｚ |

審査請求　未請求　請求項の数４　ＯＬ　（全 11 頁）

(21)出願番号　特願平7－226682

(22)出願日　平成７年(1995)９月４日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　阿部　正幸
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　斉藤　泰一
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　植田　広樹
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

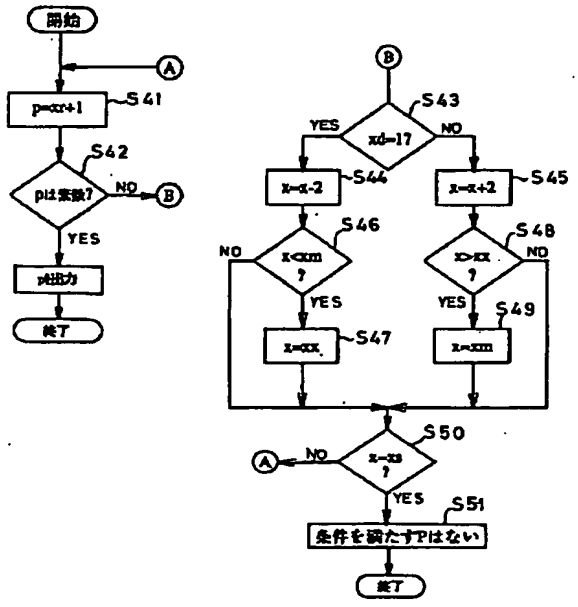
(74)代理人　弁理士　三好　秀和　（外１名）

(54)【発明の名称】　素数生成装置、素因数判定装置、および制限付き素数生成装置

(57)【要約】

【課題】　Ｐ－１，Ｐ＋１が含むべき素因数のビット数のいずれもがＰのビット数の１／２以上となるような安全性の高い素数を生成するとともに素数の出現確率が比較的均等である素数生成装置、素因数判定装置、および制限付き素数生成装置を提供する。

【解決手段】　素数ｐのビット数ｐｂ，ｐ－１の素因数とする素数ｒ，ｘの最大値ｘｘ，ｘの最小値ｘｍ，ｘの終了値ｘｓ，ｘｍ≦ｘ≦ｘｘなる偶数の乱数ｘ、および乱数ｘｄが外部より入力されたとき、ｐ＝ｘｒ＋１を計算し、ｐを素数判定器へ入力し、ｐが素数と判定された場合にｐを出力して処理を停止し、ｐが素数でないと判定された場合には、ｘｄの値に応じてｘから２を減じるかまたはｘに２を加え、ｘがｘｍより小さくなった場合はｘをｘｘとし、ｘがｘｘより大きくなった場合はｘをｘｍとし、ｘがｘｓと等しい場合には、入力条件ｐｂ，ｒを満たす素数ｐが存在しないという信号を出力して停止し、ｘがｘｓに等しくない場合には最初の処理に戻る。



【特許請求の範囲】

【請求項１】　乱数生成器および素数判定器を備え、ｒを素数、ｘを乱数とするときｐ＝ｘｒ＋１からなる素数ｐを生成する素数生成装置であって、

素数ｐのビット数ｐｂ，ｐ－１の素因数とする素数ｒ，ｘの最大値ｘｘ，ｘの最小値ｘｍ，ｘの終了値ｘｓ，ｘｍ≦ｘ≦ｘｘなる偶数の乱数ｘ、および乱数ｘｄが外部より入力されたとき、ｐ＝ｘｒ＋１を計算する第１の手段と、

ｐを前記素数判定器へ入力し、ｐが素数と判定された場合にｐを出力して処理を停止し、ｐが素数でないと判定された場合に第３の手段に処理を渡す第２の手段と、

ｘｄの値に応じてｘから２を減じるかまたはｘに２を加え、ｘがｘｍより小さくなった場合はｘをｘｘとし、ｘがｘｘより大きくなった場合はｘをｘｍとし、ｘがｘｓと等しい場合には第４の手段に処理を渡し、ｘがｘｓに等しくない場合には第１の手段に処理を渡す第３の手段と、

入力条件ｐｂ，ｒを満たす素数ｐが存在しないという信号を出力して停止する第４の手段とを有することを特徴とする素数生成装置。

【請求項２】　前記第１の手段において、ｘがｘｓまたはｘｘまたはｘｓと等しい場合にのみｐ＝ｘｒ＋１を計算し、それ以外の場合には、ｘｄの値に応じてｐに２＊ｒを加えるかまたは減じた結果をｐとすることを特徴とする請求項１記載の素数生成装置。

【請求項３】　素数ｐおよび整数ｓｂが入力された時、ｐ＋１がｓｂビット以上の素因数を持つかどうかを判定する素因数判定装置であって、

２から順番に素数を格納した記憶手段である素数テーブル、素数判定器および除算器を備え、前記素数テーブルに格納されている最大の素数をｔmax とするとき、レジスタｔを０に初期化し、ｐ＋１をレジスタｓに格納する第１の手段と、

前記素数テーブルにｔより大きな素数がある場合はそれらのうちの最小の値を読み出してｔに格納するかまたはｔより大きい素数が素数テーブルにない場合は第５の手段に処理を渡す第２の手段と、

ｓとｔを除算器へ入力し、ｓがｔで割り切れた場合に出力商をｓとして第３の手段に処理を渡すかまたはｓが割り切れなかった場合に前記第２の手段に処理を渡す第３の手段と、

ｓのビット数｜ｓ｜をカウントし、｜ｓ｜がｓｂより小さい場合にｐ＋１はｓｂビット以上の素因数を持たないとの判定結果を出力して停止するかあるいは｜ｓ｜がｓｂ以上の場合に前記第２の手段に処理を渡す第４の手段と、

前記素数判定器にｓを入力し、ｓが素数の場合はｐ＋１はｓｂビット以上の素因数を持つとの判定結果を出力するかあるいはｓが素数でない場合はｐ＋１はｓｂビット以上の素因数を持たないとの判定結果を出力して停止する第５の手段とを有することを特徴とする素因数の大きさを判定する素因数判定装置。

【請求項４】　乱数生成器および素数判定器を備え、ｒを素数、ｘを乱数とするときｐ＝ｘｒ＋１からなる素数ｐを生成する素数生成装置であって、素数ｐのビット数ｐｂ，ｐ－１の素因数とする素数ｒ，ｘの最大値ｘｘ，ｘの最小値ｘｍ，ｘの終了値ｘｓ，ｘｍ≦ｘ≦ｘｘなる偶数の乱数ｘ、および乱数ｘｄが外部より入力されたとき、ｐ＝ｘｒ＋１を計算する第１の手段、ｐを前記素数判定器へ入力し、ｐが素数と判定された場合にｐを出力して処理を停止し、ｐが素数でないと判定された場合に第３の手段に処理を渡す第２の手段、ｘｄの値に応じてｘから２を減じるかまたはｘに２を加え、ｘがｘｍより小さくなった場合はｘをｘｘとし、ｘがｘｘより大きくなった場合はｘをｘｍとし、ｘがｘｓと等しい場合には第４の手段に処理を渡し、ｘがｘｓに等しくない場合には第１の手段に処理を渡す第３の手段および入力条件ｐｂ，ｒを満たす素数ｐが存在しないという信号を出力して停止する第４の手段を有する素数生成装置と、素数ｐおよび整数ｓｂが入力された時、ｐ＋１がｓｂビット以上の素因数を持つかどうかを判定する素因数判定装置であって、２から順番に素数を格納した記憶手段である素数テーブル、素数判定器および除算器を備え、前記素数テーブルに格納されている最大の素数をｔmax とするとき、レジスタｔを０に初期化し、ｐ＋１をレジスタｓに格納する第１の手段、前記素数テーブルにｔより大きな素数がある場合はそれらのうちの最小の値を読み出してｔに格納するかまたはｔより大きい素数が素数テーブルにない場合は第５の手段に処理を渡す第２の手段、ｓとｔを除算器へ入力し、ｓがｔで割り切れた場合に出力商をｓとして第３の手段に処理を渡すかまたはｓが割り切れなかった場合に前記第２の手段に処理を渡す第３の手段、ｓのビット数｜ｓ｜をカウントし、｜ｓ｜がｓｂより小さい場合にｐ＋１はｓｂビット以上の素因数を持たないとの判定結果を出力して停止するかあるいは｜ｓ｜がｓｂ以上の場合に前記第２の手段に処理を渡す第４の手段および前記素数判定器にｓを入力し、ｓが素数の場合はｐ＋１はｓｂビット以上の素因数を持つとの判定結果を出力するかあるいはｓが素数でない場合はｐ＋１はｓｂビット以上の素因数を持たないとの判定結果を出力して停止する第５の手段を有する素因数の大きさを判定する素因数判定装置と、乱数生成器と、素数判定器とを備え、整数ｐｂ，ｒｂ，ｓｂ，ｔｂが外部より入力されたとき、ｐ－１がｒｂビットの素因数ｒを持ち、ｐ＋１がｓｂビットの素因数ｓを持ち、ｒ－１がｔｂビットの素因数を持つような素数ｐを生成する制限付き素数生成装置であって、

前記乱数生成器を駆動してｔｂビットの乱数ｔを生成する第１の手段と、

ｔを前記素数判定器に入力し、ｔが素数の場合には第３の手段に処理を渡し、ｔが素数でない場合には前記第１の手段に処理を戻す第２の手段と、

$2^{rb-1}$／ｔをｘｒｘとし、$2^{rb-1}$／ｔをｘｒｍとし、乱数生成器を駆動してｘｒｍ≦ｘｒｓ≦ｘｒｘとなるｘｒｓを生成し、レジスタｘｒをｘｒｓで初期化し、乱数生成器を駆動して乱数をｘｒｄへ格納する第３の手段と、

ビット数ｒｂ、素数ｔ、乱数ｘｒ、最大値ｘｒｘ、最小値ｘｒｍ、終了値ｘｒｓおよび乱数ｘｒｄを前記素数生成装置に入力し、素数が出力された場合はｒへ格納して第５の手段に処理を渡し、または入力条件を満たす素数が存在しないという信号が出力された場合には前記第１の手段に処理を渡す第４の手段と、

$2^{pb-1}$／ｒをｘｐｘとし、$2^{pb-1}$／ｒをｘｐｍとし、乱数生成器を駆動してｘｐｍ≦ｘｐｓ≦ｘｐｘとなる偶数のｘｐｓを生成し、レジスタｘｐをｘｐｓで初期化し、乱数生成器を駆動して出力乱数をｘｐｄへ格納する第５の手段と、

ビット数ｐｂ、素数ｒ、乱数ｘｐ、最大値ｘｐｘ、最小値ｘｐｍ、終了値ｘｐｓおよびｘｐｄを前記素数生成装置に入力し、素数が出力された場合はｐへ格納して第７の手段に処理を渡し、または入力条件を満たす素数が存在しないという信号が出力された場合は前記第４の手段に処理を戻す第６の手段と、

素数ｐと整数ｓｂを前記素因数判定装置に入力し、ｐ＋１はｓｂビットの素因数を持たないと判定された場合は前記第６の手段に処理を戻し、ｐ＋１がｓｂビットの素因数を持つと判定された場合にはｐを出力して停止する第７の手段とを有することを特徴とする制限付き素数生成装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えば情報セキュリティの分野で公開鍵暗号に用いる鍵となる素数を生成する素数生成装置、素因数判定装置、および制限付き素数生成装置に関する。

【０００２】

【従来の技術】素因数分解の困難性に基づく公開鍵暗号方式では、秘密鍵として５１２bit 程度の大きな素数を用いる。２つの素数Ｐ，Ｑの積Ｎが与えられてもＰ，Ｑを求めることが困難であれば、Ｎを公開してもＰ，Ｑを知られる恐れはない。しかし、Ｐ，Ｑの構造によっては、Ｎの素因数分解が容易になる場合がある。

【０００３】Ｎの素因数分解を困難にするために素数Ｐが満たすべき条件として、Ｘ５０９標準では次の項目を挙げている。Ｑについても同様。

【０００４】（１）Ｐ＋１が大きな素因数ｓを持つこと
（２）Ｐ－１が大きな素因数ｒを持つこと
（３）ｒ－１が大きな素因数ｔを持つこと
（４）Ｐはランダムであること

どれだけ大きければよいかは攻撃法や計算機の進歩に依存している。素数Ｐのビット数をｐｂ，Ｐ＋１の素因数ｓをｓｂビット、Ｐ－１の素因数ｒをｒｂビットとして、ｒｂ＋ｓｂ＜ｐｂの場合には以下の素数生成法を利用することが可能である。

【０００５】（ａ）ｔｂビットの素数ｔを生成
（ｂ）ｒ＝２ｘｔ＋１となるｒｂビットの素数ｒを生成
（ｃ）ｓｂビットの素数ｓを生成
（ｄ）ｒｉ＝１／ｒmod ｓを計算
（ｅ）Ｐ＝２（ｙｓ－ｒｉ）ｒ＋１となるｐｂビットの素数Ｐを生成

【０００６】

【発明が解決しようとする課題】上述した従来法では、ｒｂ＋ｓｂ＜ｐｂでなければならず、上述した（１）の条件を満たすためにｒｂを大きく取るとｓｂを小さくせざるを得ない。

【０００７】図５は従来法の詳細を示している。この従来法では、ｘやｙを＋の方向に増加させて素数を探索しているが、素数の間隔は一様でないので、一方向にだけ探索すると他の素数よりも高い確率で出現する素数が存在し得る。例えば、ｒ１＝ｘ１＊ｔ＋１，ｒ２＝ｘ２＊ｔ＋１，ｒ３＝ｘ３＊ｔ＋１なる素数ｒ１，ｒ２，ｒ３を考えると、ｘを２ずつ増加させて調べる従来法ではｘの初期値がｘの区間（ｘ２，ｘ３）に入った場合は必ずｘ３側へ向かい、結果として必ずｒ３が選ばれる。区間（ｘ１，ｘ２）よりも（ｘ２，ｘ３）の方が大きい場合、ｒ２が選ばれる確率はｒ３が選ばれる確率に比較して小さくなってしまう。（４）の条件を満たすには、生成される素数の出現確率には片寄りがないことが望ましい。

【０００８】本発明は、上記に鑑みてなされたもので、その目的とするところは、Ｐ－１，Ｐ＋１が含むべき素因数のビット数のいずれもがＰのビット数の１／２以上となるような安全性の高い素数を生成するとともに素数の出現確率が比較的均等である素数生成装置、素因数判定装置、および制限付き素数生成装置を提供することにある。

【０００９】

【課題を解決するための手段】上記目的を達成するため、請求項１記載の本発明は、乱数生成器および素数判定器を備え、ｒを素数、ｘを乱数とするときｐ＝ｘｒ＋１からなる素数ｐを生成する素数生成装置であって、素数ｐのビット数ｐｂ，ｐ－１の素因数とする素数ｒ，ｘの最大値ｘｘ，ｘの最小値ｘｍ，ｘの終了値ｘｓ，ｘｍ≦ｘ≦ｘｘなる偶数の乱数ｘ、および乱数ｘｄが外部より入力されたとき、ｐ＝ｘｒ＋１を計算する第１の手段と、ｐを前記素数判定器へ入力し、ｐが素数と判定された場合にｐを出力して処理を停止し、ｐが素数でないと判定された場合に第３の手段に処理を渡す第２の手段

と、ｘｄの値に応じてｘから２を減じるかまたはｘに２を加え、ｘがｘｍより小さくなった場合はｘをｘｘとし、ｘがｘｘより大きくなった場合はｘをｘｍとし、ｘがｘｓと等しい場合には第４の手段に処理を渡し、ｘがｘｓに等しくない場合には第１の手段に処理を渡す第３の手段と、入力条件ｐｂ，ｒを満たす素数ｐが存在しないという信号を出力して停止する第４の手段とを有することを要旨とする。

【００１０】また、請求項２記載の本発明は、請求項１記載の発明において、前記第１の手段では、ｘがｘｓまたはｘｘまたはｘｓと等しい場合にのみｐ＝ｘｒ＋１を計算し、それ以外の場合には、ｘｄの値に応じてｐに２＊ｒを加えるかまたは減じた結果をｐとすることを要旨とする。

【００１１】更に、請求項３記載の本発明は、素数ｐおよび整数ｓｂが入力された時、ｐ＋１がｓｂビット以上の素因数を持つかどうかを判定する素因数判定装置であって、２から順番に素数を格納した記憶手段である素数テーブル、素数判定器および除算器を備え、前記素数テーブルに格納されている最大の素数をｔmax とするとき、レジスタｔを０に初期化し、ｐ＋１をレジスタｓに格納する第１の手段と、前記素数テーブルにｔより大きな素数がある場合はそれらのうちの最小の値を読み出してｔに格納するかまたはｔより大きい素数が素数テーブルにない場合は第５の手段に処理を渡す第２の手段と、ｓとｔを除算器へ入力し、ｓがｔで割り切れた場合に出力商をｓとして第３の手段に処理を渡すかまたはｓが割り切れなかった場合に前記第２の手段に処理を渡す第３の手段と、ｓのビット数｜ｓ｜をカウントし、｜ｓ｜がｓｂより小さい場合にｐ＋１はｓｂビット以上の素因数を持たないとの判定結果を出力して停止するかあるいは｜ｓ｜がｓｂ以上の場合に前記第２の手段に処理を渡す第４の手段と、前記素数判定器にｓを入力し、ｓが素数の場合はｐ＋１はｓｂビット以上の素因数を持つとの判定結果を出力するかあるいはｓが素数でない場合はｐ＋１はｓｂビット以上の素因数を持たないとの判定結果を出力して停止する第５の手段とを有することを要旨とする。

【００１２】請求項４記載の本発明は、乱数生成器および素数判定器を備え、ｒを素数、ｘを乱数とするときｐ＝ｘｒ＋１からなる素数ｐを生成する素数生成装置であって、素数ｐのビット数ｐｂ，ｐ－１の素因数とする素数ｒ，ｘの最大値ｘｘ，ｘの最小値ｘｍ，ｘの終了値ｘｓ，ｘｍ≦ｘ≦ｘｘなる偶数の乱数ｘ、および乱数ｘｄが外部より入力されたとき、ｐ＝ｘｒ＋１を計算する第１の手段、ｐを前記素数判定器へ入力し、ｐが素数と判定された場合にｐを出力して処理を停止し、ｐが素数でないと判定された場合に第３の手段に処理を渡す第２の手段、ｘｄの値に応じてｘから２を減じるかまたはｘに２を加え、ｘがｘｍより小さくなった場合はｘをｘｘとし、ｘがｘｘより大きくなった場合はｘをｘｍとし、ｘがｘｓと等しい場合には第４の手段に処理を渡し、ｘがｘｓに等しくない場合には第１の手段に処理を渡す第３の手段および入力条件ｐｂ，ｒを満たす素数ｐが存在しないという信号を出力して停止する第４の手段を有する素数生成装置と、素数ｐおよび整数ｓｂが入力された時、ｐ＋１がｓｂビット以上の素因数を持つかどうかを判定する素因数判定装置であって、２から順番に素数を格納した記憶手段である素数テーブル、素数判定器および除算器を備え、前記素数テーブルに格納されている最大の素数をｔmax とするとき、レジスタｔを０に初期化し、ｐ＋１をレジスタｓに格納する第１の手段、前記素数テーブルにｔより大きな素数がある場合はそれらのうちの最小の値を読み出してｔに格納するかまたはｔより大きい素数が素数テーブルにない場合は第５の手段に処理を渡す第２の手段、ｓとｔを除算器へ入力し、ｓがｔで割り切れた場合に出力商をｓとして第３の手段に処理を渡すかまたはｓが割り切れなかった場合に前記第２の手段に処理を渡す第３の手段、ｓのビット数｜ｓ｜をカウントし、｜ｓ｜がｓｂより小さい場合にｐ＋１はｓｂビット以上の素因数を持たないとの判定結果を出力して停止するかあるいは｜ｓ｜がｓｂ以上の場合に前記第２の手段に処理を渡す第４の手段および前記素数判定器にｓを入力し、ｓが素数の場合はｐ＋１はｓｂビット以上の素因数を持つとの判定結果を出力するかあるいはｓが素数でない場合はｐ＋１はｓｂビット以上の素因数を持たないとの判定結果を出力して停止する第５の手段を有する素因数の大きさを判定する素因数判定装置と、乱数生成器と、素数判定器とを備え、整数ｐｂ，ｒｂ，ｓｂ，ｔｂが外部より入力されたとき、ｐ－１がｒｂビットの素因数ｒを持ち、ｐ＋１がｓｂビットの素因数ｓを持ち、ｒ－１がｔｂビットの素因数を持つような素数ｐを生成する制限付き素数生成装置であって、前記乱数生成器を駆動してｔｂビットの乱数ｔを生成する第１の手段と、ｔを前記素数判定器に入力し、ｔが素数の場合には第３の手段に処理を渡し、ｔが素数でない場合には前記第１の手段に処理を戻す第２の手段と、$2^{rb-1}/t$をｘｒｘとし、$2^{rb-1}/t$をｘｒｍとし、乱数生成器を駆動してｘｒｍ≦ｘｒｓ≦ｘｒｘとなるｘｒｓを生成し、レジスタｘｒをｘｒｓで初期化し、乱数生成器を駆動して乱数をｘｒｄへ格納する第３の手段と、ビット数ｒｂ、素数ｔ、乱数ｘｒ、最大値ｘｒｘ、最小値ｘｒｍ、終了値ｘｒｓおよび乱数ｘｒｄを前記素数生成装置に入力し、素数が出力された場合はｒへ格納して第５の手段に処理を渡し、または入力条件を満たす素数が存在しないという信号が出力された場合には前記第１の手段に処理を渡す第４の手段と、$2^{pb-1}/r$をｘｐｘとし、$2^{pb-1}/r$をｘｐｍとし、乱数生成器を駆動してｘｐｍ≦ｘｐｓ≦ｘｐｘとなる偶数のｘｐｓを生成し、レジスタｘｐをｘｐｓで初期化し、乱数生成器を駆動して

出力乱数をｘｐｄへ格納する第５の手段と、ビット数ｐｂ、素数ｒ、乱数ｘｐ、最大値ｘｐｘ、最小値ｘｐｍ、終了値ｘｐｓおよびｘｐｄを前記素数生成装置に入力し、素数が出力された場合はｐへ格納して第７の手段に処理を渡し、または入力条件を満たす素数が存在しないという信号が出力された場合は前記第４の手段に処理を戻す第６の手段と、素数ｐと整数ｓｂを前記素因数判定装置に入力し、ｐ＋１はｓｂビットの素因数を持たないと判定された場合は前記第６の手段に処理を戻し、ｐ＋１がｓｂビットの素因数を持つと判定された場合にはｐを出力して停止する第７の手段とを有することを要旨とする。

【００１３】本発明では、最初に上述した条件（２），（３）を満たす素数Ｐを生成し、次いでその素数が上述した条件（１）を満たすかどうかを高速に確認する。また、素数Ｐを探索する場合には探索の方向を乱数によって決定する。

【００１４】まず、素数生成装置は、生成する素数ｐのビット数ｐｂ，ｐ－１の素因数とする素数ｒ，ｘの最大値ｘｘ，ｘの最小値ｘｍ，ｘの終了値ｘｓ，ｘｍ≦ｘ≦ｘｘなる偶数の乱数ｘ、および乱数ｘｄを外部より受け付けて、ｐ＝ｘｒ＋１を計算してｐを素数判定器へ入力し、ｐが素数でない場合にはｘｄの値に応じて、ｘから２を減じるかまたはｘに２を加え、その結果ｘがｘｍより小さくなった場合はｘをｘｘとし、ｘがｘｘより大きくなった場合はｘをｘｍとする。また、ｘがｘｓと等しくなった場合には、入力条件ｐｂ，ｒを満たす素数ｐが存在しないという信号を出力して停止する。ｘがｘｓと等しくならなかった場合は、再びｐ＝ｘｒ＋１を計算して素数判定を行い、ｐが素数となるまでこれを繰り返すように構成する。

【００１５】次に、乱数生成器と素数判定器を繰り返し用いてｔｂビットの素数ｔを生成する。素数ｔが得られたら、ｘｘ＝（$2^{rb}-1$）／ｔ，ｘｍ＝$2^{rb-1}$／ｔとしてｘの最大値ｘｘと最小値ｘｍを求める。乱数生成器を駆動してｘｍ≦ｘｓ≦ｘｘなる偶数の乱数ｘｓを生成し、ｘをｘｓで初期化する。更に乱数生成器を駆動して乱数ｘｄを得る。これらｒｂ，ｔ，ｘｘ，ｘｍ，ｘｓ，ｘ，ｘｄを素数生成装置へ入力し、ｒｂビットの素数ｒを得る。

【００１６】素数ｒが得られたら、同様にしてｒからＰを生成する。ｙｘ＝（$2^{pb}-1$）／ｒ，ｙｍ＝$2^{pb-1}$／ｒとしてｙの最大値ｙｘと最小値ｙｍを求める。乱数生成器を駆動してｙｍ≦ｙｓ≦ｙｘなる偶数の乱数ｙｓを生成し、ｙをｙｓで初期化する。更に乱数生成器を駆動して乱数ｙｄを得る。ｐｂ，ｒ，ｙｘ，ｙｍ，ｙｓ，ｙ，ｙｄを素数生成装置へ入力し、ｐｂビットの素数Ｐを得る。

【００１７】最後に、Ｐ＋１がｓｂビット以上の大きな素因数ｓを持つかどうかを判定する。適当なビット数以下の素数を全て格納した素数テーブルを予め作っておく。まずｋを０に、ｓをＰ＋１に初期化する。

【００１８】ｋより大きな最小の素数を素数テーブルから読み出してｋに格納する。ｓがｋで割り切れる場合はｓをｔで割り切れなくなるまで繰り返して割る。ｓがｓｂビットより小さくなってしまったら、Ｐ＋１は大きな素因数を持たないことを意味するので、Ｐの生成をやり直す。テーブル中の素数全てについてｓに対する除算を試しても、ｓがｓｂビットより大きい場合は、ｓが大きな素因数かどうかを素数判定器にｓを入力して判定する。ｓが素数でない場合は、Ｐの生成をやり直す。ｓが素数の場合は、Ｐ＋１がｓｂビット以上の大きな因数ｓを含んでいるので、Ｐを条件を満たす素数として出力する。

【００１９】以上の手段により、ｘ，ｙを増加させるか、減少させるかを乱数によって決定することで、よりランダムな素数を生成することができる。

【００２０】また、ｘ，ｙをｒ，Ｐ生成後も保持しておき、ｒまたはＰが条件に合わない素数であった場合に、ｘ，ｙの探索を最初からやり直すのではなく、更新を再開してｒまたはＰを探索するようにすることでｔやｓを生成し直す時間を削除できる。

【００２１】Ｐ＋１を小さな素数で可能なかぎり除した後、素数判定器へ入力することによって、ｒｂの値に制約を受けない大きなビット数ｓｂの素因数ｓを含むＰ＋１なる素数Ｐを検出することができる。

【００２２】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【００２３】図１は、本発明の一実施形態の構成を示すブロック図であり、図２は、図１に示す実施形態に使用されている素数生成装置の構成を示すブロック図である。

【００２４】図１に示す実施形態は、乱数生成器１１、素数判定器１３、除算器１５、乱数発生器２１、素数生成装置１７、除算器２５、乱数生成器３１、素数生成装置２７、除算器３５、素数テーブル１９、素数判定器２３を有する。また、図２に示す素数生成装置は、乗算器、加算器、減算器、比較器からなる算術演算回路（以下、ＡＬＵと略称する）４１、素数判定器４３、乗数ｘの値を更新する乗数更新部４５を有する。

【００２５】まず、図４を参照して、図２に示す素数生成装置の作用を説明する。

【００２６】図２および図４において、生成する素数ｐのビット数ｐｂ，ｐ－１の素因数とする素数ｒ，ｘの最大値ｘｘ，ｘの最小値ｘｍ，ｘの終了値ｘｓ，ｘｍ≦ｘ≦ｘｘなる偶数の乱数ｘ、および１bit の乱数ｘｄを外部より受け付けて、ＡＬＵ４１を駆動してｐ＝ｘ＊ｒ＋１を計算し、ｐを素数判定器４３へ入力する（ステップＳ４１）。ｐが素数でない場合には（ステップＳ４２）

乗数更新部４５を駆動してｘを更新する。ｘの更新はｘｄが１の時ｘにｘ－２を格納し（ステップＳ４３，Ｓ４４）、またはｘｄが０の時ｘにｘ＋２を格納する（ステップＳ４３，Ｓ４５）。その結果ｘがｘｍより小さくなった場合はｘをｘｘとし、ｘがｘｘより大きくなった場合はｘをｘｍとする（ステップＳ４６～Ｓ４９）。また、ステップＳ５０でｘがｘｓと等しくなった場合には、入力条件ｐｂ，ｒを満たす素数ｐが存在しないという信号を出力して停止する（ステップＳ５１）。ｘがｘｓと等しくならなかった場合は、再びｐ＝ｘ＊ｒ＋１を計算して素数判定を行い、ｐが素数となるまでこれを繰り返し、素数ｐが得られたらこれを出力して停止する構成とする。

【００２７】まず、乱数生成器１１の４８０bit の乱数出力ｔを素数判定器１３へ入力する（ステップＳ１１）。素数となるｔが得られるまで繰り返し行う（ステップＳ１２）。素数ｔが得られたら、除算器１５へ$2^{496}-1$とｔを入力してその出力をｘｘとし、ｘｘ＝［（$2^{496}-1$）／ｒ］を得る。ここで、［ａ］はａを越えない最大の整数を表す記号とする。同様に、除算器１５へ$2^{495}$とｔを入力して出力をｘｍとし、ｘｍ＝［$2^{495}$／ｒ］を得る（ステップＳ１３）。続いて、乱数生成器２１を駆動し、ｘｍ≦ｘｓ≦ｘｘとなるｘｓを生成し、ｘにｘｓを格納する。また、乱数生成器２１を駆動し、その出力の最下位１bit の値をｘｄへ格納する（ステップＳ１４）。

【００２８】４９６，ｘｘ，ｘｍ，ｘｓ，ｘ，ｘｄを素数生成装置１７へ入力し、４９６bit の素数ｒを得る（ステップＳ１５）。素数生成装置１７が入力条件を満たす素数が存在しないという信号を出力した場合は、ｔの生成をやり直す（ステップＳ１６）。

【００２９】素数ｒが得られたら、除算器２５へ$2^{512}-1$とｔを入力してその出力をｙｘとし、ｘｙ＝［（$2^{512}-1$）／ｒ］を得る。同様に、除算器２５へ$2^{511}$とｒを入力して出力をｙｍとし、ｙｍ＝［$2^{511}$／ｒ］を得る（ステップＳ１７）。続いて、乱数生成器３１を駆動し、ｙｍ≦ｙｓ≦ｙｘとなるｙｓを生成し、ｙにｙｓを格納する。また、乱数生成器を駆動し、その出力の最下位１bit の値をｙｄへ格納する（ステップＳ１８）。

【００３０】５１２，ｙｘ，ｙｍ，ｙｓ，ｙ，ｙｄを素数生成装置２７へ入力し、５１２bit の素数Ｐを得る（ステップＳ１９）。素数生成装置２７が入力条件を満たす素数が存在しないという信号を出力した場合は、ｓの生成をやり直す（ステップＳ２０）。

【００３１】素数Ｐが得られたら、Ｐ＋１が４９６bit 以上の素因数ｓを含んでいるかどうかを判定する。８ビット以下の素数を全て格納した素数テーブルを予め作っておく。

【００３２】まず、ｋを０に、ｓをＰ＋１に初期化する。ｋより大きな最小の素数（＝２）を素数テーブルから読み出してｋに格納する（ステップＳ２１）。ｓがｋで割り切れる場合はｓをｔで割り切れなくなるまで繰り返して割る。ｓが４９６bit より小さくなってしまったら、Ｐ＋１は４９６bit 以上の素因数を持たないことを意味するので、Ｐの生成をやり直す（ステップＳ２２～Ｓ２６）。テーブル中の素数全てについてｓに対する除算を試しても、ｓがｓｂビットより大きい場合は、ｓが大きな素因数かどうかを素数判定器２３にｓを入力して判定する。ｓが素数でない場合は、Ｐの生成をやり直す。ｓが素数の場合は、Ｐ＋１がｓｂビット以上の大きな因数ｓを含んでいるので、Ｐを条件を満たす素数として出力する（ステップＳ２７）。

【００３３】

【発明の効果】以上説明しように、本発明によれば、素数Ｐのビット数をｐｂ，Ｐ－１が含むべき素因数のビット数をｒｂ，Ｐ＋１が含むべき素因数のビット数をｓｂとして、ｒｂ，ｓｂがともに大きな場合にもｒｂビットの素因数をＰ－１が含み、ｓｂビットの素因数をＰ＋１が含むようなｐｂビットのランダムな素数Ｐを効率よく生成することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態の構成を示すブロック図である。

【図２】図１に示す実施形態に使用されている素数生成装置の構成を示すブロック図である。

【図３】図１に示す実施形態の作用を示すフローチャートである。

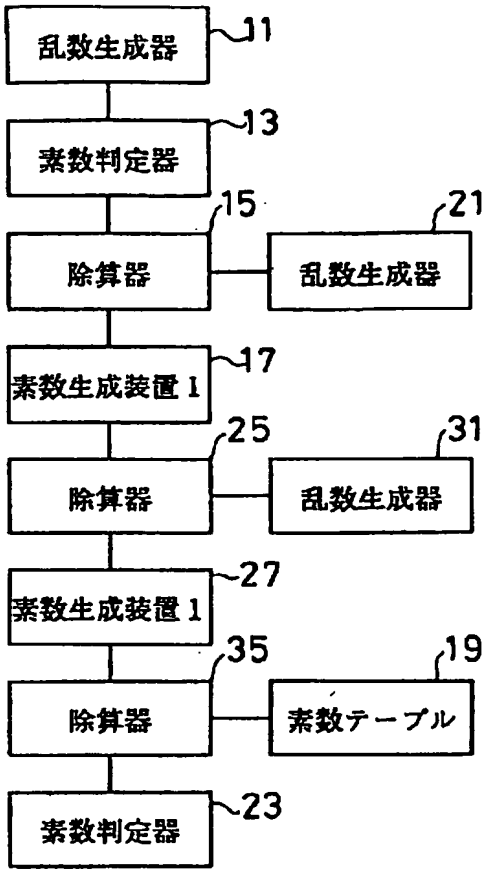
【図４】図２に示す素数生成装置の作用を示すフローチャートである。

【図５】従来法の作用を示すフローチャートである。

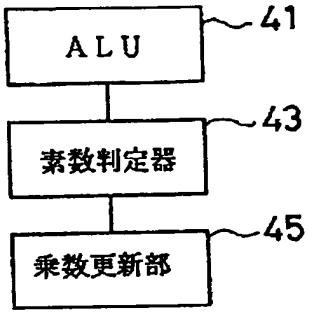
【符号の説明】

１１，２１，３１　乱数生成器
１３，２３，４３　素数判定器
１５，２５，３５　除算器
１７，２７　素数生成装置
１９　素数テーブル
４１　ＡＬＵ
４５　乗数更新部

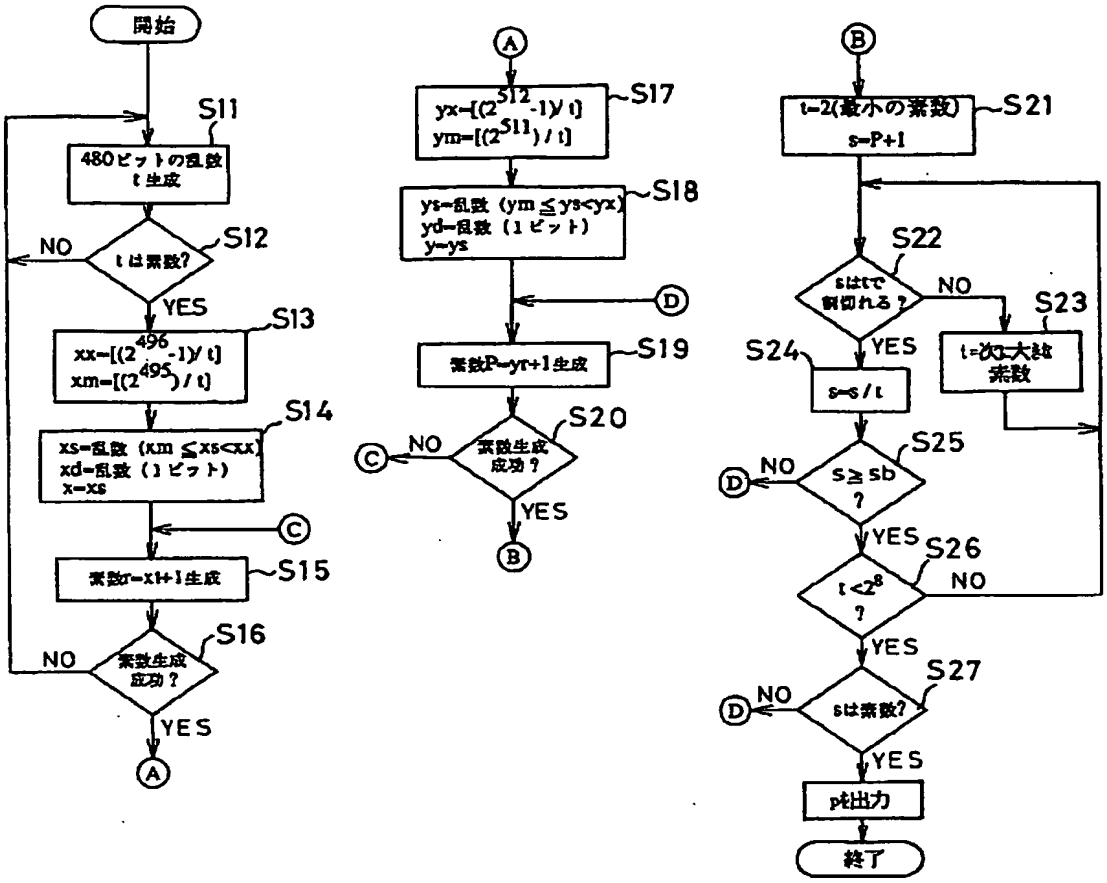
【図１】


乱数生成器
11
素数判定器
13
除算器
15
乱数生成器
21
素数生成装置１
17
除算器
25
乱数生成器
31
素数生成装置１
27
除算器
35
素数テーブル
19
素数判定器
23

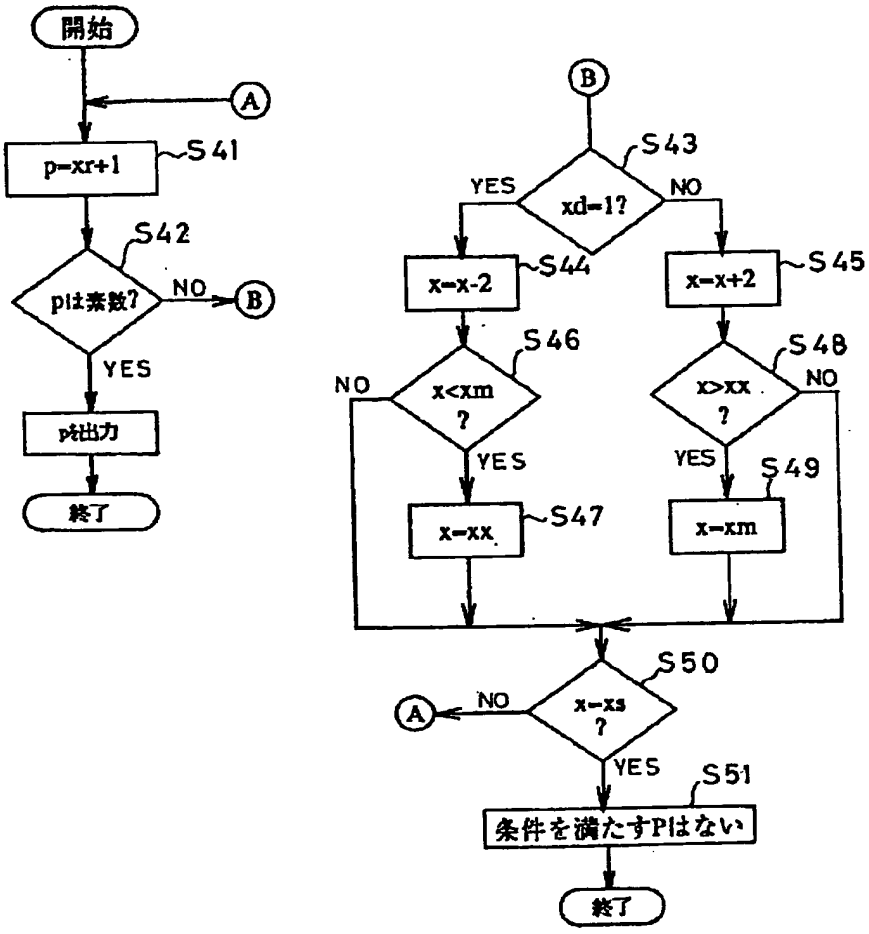
【図２】



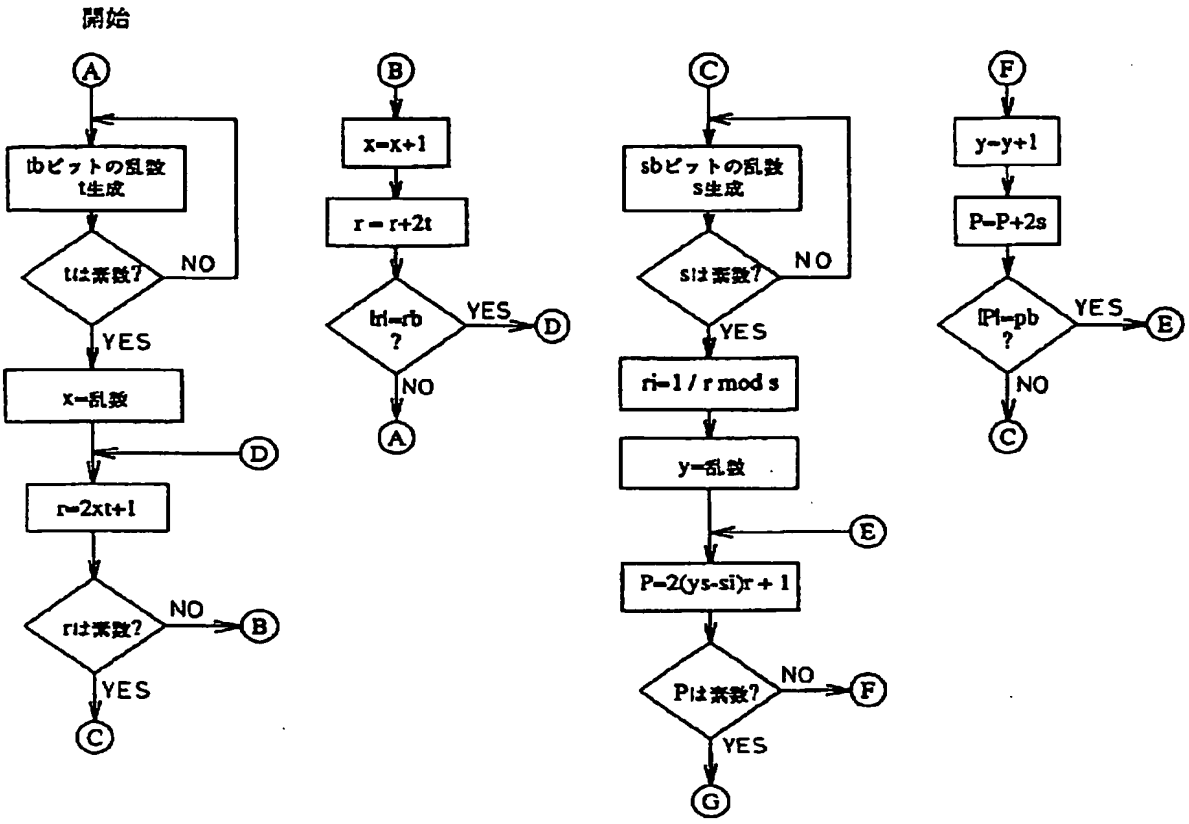
【図３】


開始
S11
480ビットの乱数t生成
S12
tは素数?
NO
YES
S13
xx=[(2^496-1)/t]
xm=[(2^495)/t]
S14
xs=乱数 (xm≦xs<xx)
xd=乱数 (1ビット)
x=xs
C
S15
素数r=xt+1生成
S16
素数生成成功?
NO
YES
A
A
S17
yx=[(2^512-1)/t]
ym=[(2^511)/t]
S18
ys=乱数 (ym≦ys<yx)
yd=乱数 (1ビット)
y=ys
D
S19
素数P=yr+1生成
S20
素数生成成功?
NO
C
YES
B
B
S21
t=2(最小の素数)
s=P+1
S22
sはtで割切れる?
NO
YES
S23
t=次に大きな素数
S24
s=s/t
S25
s≧sb?
NO
D
YES
S26
t<2^8?
NO
YES
S27
sは素数?
NO
D
YES
p,t出力
終了

【図４】


開始
A
p=xr+1
S41
S42
pは素数?
NO
B
YES
pを出力
終了
B
S43
YES
xd=1?
NO
x=x-2
S44
x=x+2
S45
S46
S48
NO
x<xm
?
x>xx
?
NO
YES
YES
S49
x=xx
S47
x=xm
S50
A
NO
x=xs
?
YES
S51
条件を満たすPはない
終了

【図５】


開始
A
bビットの乱数 t生成
tは素数?
NO
YES
x=乱数
D
r=2xt+1
rは素数?
NO
B
YES
C
B
x=x+1
r=r+2t
|r1-rb ?
YES
D
NO
A
C
sbビットの乱数 s生成
sは素数?
NO
YES
ri=1/r mod s
y=乱数
E
P=2(ys-si)r+1
Pは素数?
NO
F
YES
G
F
y=y+1
P=P+2s
|P1-pb ?
YES
E
NO
C